Vernehmlassungsantwort

über die Änderung des Schweizerischen Strafgesetzbuches betreffend die strafrechtliche Verantwortlichkeit der Provider und die Kompetenzen des Bundes bei der Verfolgung strafbarer Handlungen mittels elektronischer Kommunikationsnetze

Swiss Internet User Group SIUG

http://www.siug.ch/

30.April 2005

Über die SIUG

Die SIUG ist eine Non-Profit-Organisation, die sich aus Internetexperten verschiedener Stufen zusammensetzt. Dazu gehören Akademiker aus verschiedenen Fachgebieten, Experten aus dem ISP-Bereich, selbständige Informatiker und Anwender. Das Ziel der SIUG ist es, sich für eine vernünftige Anwendung, Entwicklung und Reglementierung des Internets und verwandter Technologien einzusetzen, ohne dabei den ursprünglichen offenen Geist und die Tradition des Mediums übermässig einzuschränken.

Kontakt

SIUG
Postfach 1908
8021 Zürich
siug@siug.ch

Kontaktperson für Fragen zu dieser Vernehmlassungsantwort:
Matthias Leisi, matthias.leisi@siug.ch, Telefon 043 211 03 55 / 079 207 31 08

Allgemein

Die SIUG begrüsst grundsätzlich, dass im Bereich der strafrechtlichen Verantwortlichkeit der Provider eine gewisse Rechtssicherheit und -klarheit geschaffen werden soll.

Was die verschiedenen Unterlagen des Vernehmlassungsverfahrens als "Netzwerkkriminalität" bezeichnen, sind keine prinzipiell neuen Formen der Kriminalität, sondern lediglich herkömmliche Taten (beispielsweise Betrug, Erpressung etc), die *auch* über elektronische Kommunikationsmittel begangen werden.

Insofern geht es im Kern der vorliegenden StGB-Revision um die Behebung von angenommenen Vollzugsproblemen seitens der Strafverfolgungsbehörden.

Abgrenzung Inhalts- und technische Provider

Der vorliegende Entwurf ist zwar vordergründig technologieneutral, beschränkt sich in der Ausgestaltung aber praktisch ausschliesslich auf das HTTP-Modell der Informationsübertragung ("das Web"). Andere Modelle (1:1- bis m:n-Kommunikation via E-Mail, Instant Messaging oder Usenet) werden gänzlich ausser Acht gelassen. Das ist insofern bedauerlich, als dass eine grosse Masse krimineller Handlungen heute via E-Mail oder Instant Messaging zumindest initiiert werden (zB Bewerbung von gefälschten Produkten, nicht zugelassenen Arzneimitteln und nach Schweizer Recht illegalen Lotterien via E-Mail).

Die Vernehmlassung unterscheidet drei Kategorien von Providern: Content-, Hosting- und Access-Provider. Diese Kategorisierung greift zu kurz, da es noch mindestens zwei weitere Kategorien zu unterscheiden gilt:

- Housing-Provider stellen Platz und Logistik in einem Rechenzentrum sowie eine Netzwerkverbindung zur Verfügung.

- Backbone-Provider verbinden die Netzwerke verschiedener Access-, Hosting- und Housing-Provider miteinander und stellen durch sog. Peering die weitgehende globale Vernetzung zur Verfügung.

Housing-Provider sind insofern speziell zu Berücksichtigen, da diese in aller Regel keinen Zugriff auf die Daten der bei ihnen abgestellten Rechner sondern lediglich physischen Zugriff auf diese Rechner besitzen.

Die Kategorisierung der verschiedenen Provider unterschlägt indessen die Tatsache, dass "im Internet" jeder Teilnehmer prinzipbedingt immer gleichzeitig Empfänger und Sender ist. Ein Anwender kann explizit zum Sender werden, indem er beispielsweise einen Webserver auf einem über ADSL angeschlossenen Computer betreibt. Die Sender-Rolle kann auch implizit übernommen werden, sofern das im verwendeten Protokoll einer Anwendung vorgesehen ist (wie etwa beim Internet-Telefonie-Dienst Skype oder beim Peer-to-Peer-Dienst Freenet).

In diesen Fällen wäre eine erhöhte strafrechtliche Verantwortlichkeit ungebührlich. Statt auf einer künstlichen Kategorisierung abzustellen, sollte auf den der jeweiligen Netzwerktopologie zugrundeliegenden organisatorisch-administrativen Einflussbereich abgestellt werden. Im Internet könnte dies auf der Ebene der (hierarchischen) Delegation von IP-Adressblöcken geschehen.

Die SIUG ist der Meinung, dass eine klare Abgrenzung in Inhalts- und technische Provider vorgenommen werden muss. Jede andere Kategorisierung ist wegen schwammiger Begrifflichkeiten in der Praxis zum Scheitern prädestiniert.

Abgrenzung zum Medienstrafrecht

Der Bundesrat ist der Meinung, dass das Medienstrafrecht nicht anwendbar ist (ausser für eigentliche Medienschaffende). Die SIUG weist darauf hin, dass durch die vorliegende Revision in diesem Bereich eine beträchtliche Rechtsunsicherheit geschaffen wird, da die Grenzen zwischen Medienschaffenden und Internet-Benutzern zunehmend unschärfer werden. Beispielsweise dürften einige Weblogs faktisch als Medien gelten, während gleichzeitig etablierte Medienunternehmen verschiedene Formen öffentlicher Interaktivität von und mit ihren Nutzern ermöglichen.

Strafrechtliche Verantwortlichkeit der Provider (Vorentwurf A)

Angesichts der Vielzahl von konzeptionellen Unschärfen, des geringen Nutzens und der potentiell weitreichenden Folgen von strafrechtlichen Regelungen ist es aus Sicht der SIUG notwendig, die vorgeschlagene Revision des Strafgesetzbuches auf das für die Behebung der Vollzugsprobleme notwendige Minimum zu beschränken.

Artikel 14 Absatz 4 BÜPF beseitigt im Zusammenhang mit dem Entscheid der Rekurskommission des UVEK vom 27. April 2004 praktisch alle technischen und datenschützerischen Hindernisse für Strafverfolgungsbehörden in Bezug auf Netzwerkkriminalität. Daher ist es fraglich, ob die vorliegende Revision des Strafgesetzbuches überhaupt durchgeführt werden soll.

Insbesondere ist es zweifelhaft, ob mit der vorliegenden Revision für die Provider - und damit mittelbar für die Kunden - tatsächlich die Rechtssicherheit erhöht wird. Die SIUG beurteilt die Wirksamkeit der vorgeschlagenen Regelung (Fragekatalog 1.2) als insgesamt gering.

Die SIUG lehnt den "Google-Artikel" Art. 27 Absatz 3 VE-StGB ab. Die Regelung ist in Verbindung mit Art. 322bis Ziffer 1 VE-StGB nicht verhältnismässig. Die Erfahrung mit dem us-amerikanischen Digital Millenium Copyright Act (DMCA), der eine ähnliche vereinfachte Anzeigemöglichkeit an Provider mit Handlungspflicht seitens der Provider verknüpft, sollten Warnung genug sein, solch ein Instrument im Schweizer Rechtssystem nicht einführen zu wollen. Ebenso als Warnung sollte das in Deutschland grassierende Abmahnunwesen dienen. Anstelle einer ausführlichen Erläuterung verweisen wir an dieser Stelle auf das “Chilling Effects Clearinghouse” http://www.chillingeffects.org/, eine Initiative der Electronic Frontier Foundation und der Universitäten von Harvard, Stanford, Berkeley sowie weiterer akademischer Institutionen, welche die missbräuchliche Anwendung solcher Rechtsmittel dokumentiert.

Die Melde- bzw. Anzeigepflicht nach dem vorgesehenen Artikel 322bis Ziffer 1 Absatz 2 VE-StGB ist rundweg abzulehnen. Ein Provider (man erinnere sich - jeder Nutzer selbst kann auch Provider sein) ist keine Strafverfolgungsbehörde und kann keine hoheitlichen Aufgaben wahrnehmen. Für die Entgegennahme von Strafanzeigen gibt es definierte Wege, und eine formlose Mitteilung an einen Provider erscheint da weder zweck- noch verhältnismässig, sondern schlicht überflüssig.

Da davon auszugehen ist, dass eine Mehrheit der Anwender nicht in der Lage ist, den eigentlich zuständigen Provider zu ermitteln, ist davon auszugehen, dass Schweizer Provider mit einer Vielzahl von unvollständigen und/oder schlicht irreführenden Meldungen zu kämpfen haben wird.

Die Erläuterungen des Bundesrates empfehlen einem "vorsichtige[n] Hosting-Provider, sämtliche eingehenden Hinweise an die Strafverfolgungsbehörden weiter[zuleiten]". Wenn die Strafverfolgungsbehörden am gesamten Mailverkehr der Abuse-Desks der Provider interessiert sind, sollte das rechtsstaatlich transparent durch eine Überwachung gemäss BÜPF sichergestellt werden und nicht über eine versteckte, auslegungsbedürftige Spezialklausel.

Die vorgeschlagene Regelungen schweigt sich darüber aus, in welcher Form solche Hinweise an Provider erfolgen sollen. Nach täglicher Erfahrung wird dabei wahrscheinlich E-Mail die häufigste Form sein. Aufgrund der prinzipbedingten Unzuverlässigkeit von E-Mail (es gibt keine garantierte Methode, um die Zur-Kenntnisnahme eindeutig festzustellen) scheidet diese Form für Mitteilungen von solcher Wichtigkeit und Tragweite von vornherein aus.

Die Löschung gemäss Ziffer 1 Absatz 5 von Artikel 322bis VE-StGB ist zu wenig deutlich formuliert. Es leuchtet ein, dass eine Partei, soweit technisch möglich und zumutbar, auf eine entsprechende Aufforderung hin genau spezifizierte Informationen löscht beziehungsweise entfernt. An die Form der Aufforderung sind hohe Anforderungen zu stellen, um die missbräuchliche Anwendung dieser Bestimmung zu erschweren.

Weitergehende strafrechtliche Vorschriften

Der vorliegende Entwurf schweigt sich zu eigentlichen, netzwerkspezifischen kriminellen Handlungen aus. In der täglichen Praxis relevante Handlungen sind beispielsweise:

- Der Versand von Viren/Würmern, welche befallene Computer zum Versand von Spam missbrauchbar machen.
- Denial of Service Attacken, bei denen einzelne Computer oder ganze Netze mit Anfragen überflutet werden, um sie "vom Netz abzuschneiden".
- Sogenanntes "Phishing", bei welchem Nutzer zur Eingabe von Passwörtern (etwa für das Onlinebanking) auf gefälschten Seiten verleitet werden (sollen).
- Sogenanntes "SMTP Harvesting", durch welches Mailserver systematisch auf gültige Adressen abgeprüft werden und bei betroffenen Mailservern der legitime Mailverkehr behindert wird.

Solche Taten werden auch über Schweizer Internet-Zugänge verübt. Nach Ansicht der SIUG liegt *hier* der grösste Handlungsbedarf in strafrechtlicher Hinsicht. Es handelt sich einerseits um Vollzugsprobleme (das Interesse und die technische Kompetenz der Strafverfolgungsbehörden hält sich in Grenzen) sowie um ein Skalierungsproblem (der Schaden für einzelne Betroffene ist in der Regel gering, allerdings werden in der Summe sehr bedeutende Schäden angerichtet).

Es gibt sogar Provider, die solches Tun seitens ihrer Mitarbeiter dulden. *Hier* wäre eine strafrechtliche Haftung für Provider sinnvoll, verhältnismässig und effektiv, zumindest sofern Provider (als Gehilfen) und Täter sich in der Schweiz befinden (wofür viele Anzeichen sprechen).

Wenn die Schweiz über ein entsprechendes strafrechtliches Instrumentarium verfügt, wird damit auch die internationale Rechtshilfe für die organisierte Netzwerkkriminalität ermöglicht und erleichtert.

Die SIUG möchte an dieser Stelle keine detaillierten Vorschläge unterbreiten, ist aber gerne bereit, an einer Formulierung mitzuwirken.